



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/527,814	03/14/2005	Jarmo Talvitie	3502-1075	4622
<small>466</small> YOUNG & THOMPSON 209 Madison Street Suite 500 ALEXANDRIA, VA 22314			<small>7590</small> EXAMINER AVERY, JEREMIAH L.	
			<small>08/17/2009</small> ART UNIT 2431	PAPER NUMBER
			MAIL DATE 08/17/2009	DELIVERY MODE PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary

Application No.

10/527,814

Applicant(s)

TALVITIE, JARMO

Examiner

JEREMIAH AVERY

Art Unit

2431

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
 - If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
 - Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 26 May 2009.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-6, 8-10, 12, 14-23, 26, 29-31, 33, 34, 37, 40 and 41 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-6, 8-10, 12, 14-23, 26, 29-31, 33, 34, 37, 40 and 41 is/are rejected.
- 7) ☒ Claim(s) 22 and 23 is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 14 March 2005 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-846)
- 3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date _____
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: _____

DETAILED ACTION

- I. Claims 1-6, 8-10, 12, 14-23, 26, 29-31, 33, 34, 37, 40 and 41 have been examined.
- II. Responses to Applicant's remarks have been given.

Claim Rejections - 35 USC § 102

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1, 2, 8, 10, 12, 14, 18, 22, 23, 26, 29, 31, 33 and 37 are rejected under 35 U.S.C. 102(b) as being anticipated by United States Patent No. 5,842,002 to Schnurer et al., hereinafter Schnurer.

1. Regarding claim 1, Schnurer a security system comprising:
a first sub-system configured to detect in said first sub-system an unknown malicious software having a characteristic unknown to said first sub-system, and said first sub-system being configured, to perform a partial simulation in said first sub-system for activating the unknown malicious software having the characteristic unknown to said first sub-system for causing a consequence of an activation of the unknown malicious software in said first sub-system and thereafter to detect the activated unknown malicious software in said first sub-system by detecting the consequence of the activation of the unknown malicious software in said first sub-system (column 6, lines 63-67 and column 7, lines 1-18, "data is put into the emulation chamber 48 where the virus is fooled into acting as if it were really present on the host system. It is desired that any disruptive behavior the virus is capable of displaying take place in emulation

chamber 48 such as replicating, attacking another program or destroying data" and lines 48-52).

[The claimed "partial simulation" is broadly interpreted by the Examiner to pertain to the utilization of the "emulation chamber 48" within Schnurer since the virus detection means occur not within the actual host system, but within this particular virtual environment.]

2. Regarding claim 2, Schnurer discloses the security system in accordance with claim 1, configured to forward an alarm caused by the detection of the malicious software to at least one system connected to the security system (Figures 1 and 6C, column 8, lines 27-35, "Upon detection of a virus by the analysis and detection means 50, response/alarm means 52 can execute any number of user definable optional commands such as messaging or beeping a system administrator, notifying the sender and receiver of the file or program, deleting the file..." and lines 50-59).
3. Regarding claim 8, Schnurer discloses wherein the alarm is a message or at least a part of a message that is forwarded to the recipient prior to other communications (Figures 1 and 6C, column 8, lines 27-35, "Upon detection of a virus by the analysis and detection means 50, response/alarm means 52 can execute any number of user definable optional commands such as messaging or beeping a system administrator, notifying the sender and receiver of the file or program, deleting the file..." and lines 50-59).
4. Regarding claim 10, Schnurer discloses wherein the alarm is forwarded via a separate connection (column 7, lines 25-37, "trapping device 10 splits the data into two

paths", column 8, lines 27-35, "Upon detection of a virus by the analysis and detection means 50, response/alarm means 52 can execute any number of user definable optional commands such as messaging or beeping a system administrator, notifying the sender and receiver of the file or program, deleting the file..." and lines 50-59).

5. Regarding claim 12, Schnurer discloses wherein the consequence of activation of the malicious software detected by the first sub-system includes *at least one of*: a change takes place in the first sub-system prior to actions causing changes carried out by the first sub-system, a change takes place in the first sub-system that is not an action taken by the first sub-system to detect the malicious software, a message leaves for another system without command from the first sub-system, a message leaves for another system to a wrong address or to a system which no communication has been directed to, and a message does not leave for another system although it has been sent there (column 6, lines 63-67 and column 7, lines 1-18, "data is put into the emulation chamber 48 where the virus is fooled into acting as if it were really present on the host system. It is desired that any disruptive behavior the virus is capable of displaying take place in emulation chamber 48 such as replicating, attacking another program or destroying data" and lines 48-67, "The first step is to determine whether the IRQ table was modified. The second step is to determine if another program was written to." and "It is the combination of grabbing one or more IRQs and attempting changes to either the FAT or executables that allows virus activity to be detected").

6. Regarding claim 14, Schnurer discloses wherein the first sub-system chooses *one or more of* the following logics when trying to activate the malicious software:

one defined by the user, pre-programmed or at least partially random logic (column 8, lines 27-35, "Upon detection of a virus by the analysis and detection means 50, response/alarm means 52 can execute any number of *user definable optional commands* such as messaging or beeping a system administrator, notifying the sender and receiver of the file or program, deleting the file...").

7. Regarding claim 18, Schnurer discloses the security system in accordance with claim 1, that examines messages forwarded through the security system in order to detect known malicious software (column 7, lines 48-67 and column 8, lines 3-14, "allowing a virus to be detected by its 'signature'").

8. Regarding claim 22, Schnurer teaches a method for repelling a malicious software, the method being carried out in a security system including a first sub-system for forwarding messages and that is configured to detect an unknown malicious software having a characteristic unknown to said first sub-system and that is isolatable from the remainder of the security system (), the method includes the steps: detecting in said first sub-system the unknown malicious software having a characteristic unknown to said first sub-system, performing a partial simulation in said first sub-system for activating the unknown malicious software having the characteristic unknown to said first sub-system to cause a consequence of the activation in said first sub-system, monitoring functions of the security system by the first sub-system in order to detect the consequence of the activation in said first sub-system, in the partial simulation, of the unknown malicious software (column 6, lines 63-67 and column 7, lines 1-18, "data is put into the emulation chamber 48 where the virus is fooled into

acting as if it were really present on the host system. It is desired that any disruptive behavior the virus is capable of displaying take place in emulation chamber 48 such as replicating, attacking another program or destroying data" and lines 48-52),

the consequence of activation including *at least one of* the following:

a change takes place in the first sub-system prior to actions causing changes carried out by the first sub-system, a change takes place in the first sub-system that is not an action taken by the first sub-system to detect a malicious software, a message leaves for another system without command from the first sub-system, a message leaves for another system to a wrong address or to a system which no communication has been directed to, and a message does not leave for another system although it has been sent there, thereafter detecting in said first sub-system the unknown malicious software by detecting one of the consequences in said first subsystem (column 6, lines 63-67 and column 7, lines 1-18, "data is put into the emulation chamber 48 where the virus is fooled into acting as if it were really present on the host system. It is desired that any disruptive behavior the virus is capable of displaying take place in emulation chamber 48 such as replicating, attacking another program or destroying data" and lines 48-67, "The first step is to determine whether the IRQ table was modified. The second step is to determine if another program was written to." and "It is the combination of grabbing one or more IRQs and attempting changes to either the FAT or executables that allows virus activity to be detected"), and giving an alarm (Figures 1 and 6C, column 8, lines 27-35, "Upon detection of a virus by the analysis and detection means 50, response/alarm means 52 can execute

any number of user definable optional commands such as messaging or beeping a system administrator, notifying the sender and receiver of the file or program, deleting the file..." and lines 50-59).

9. Regarding claim 23, Schnurer teaches a method for repelling a malicious software, the method comprising the steps of:

detecting in a first sub-system of a security system an unknown malicious software having a characteristic unknown to said first sub-system; performing a partial simulation in the first sub-system to activate the detected unknown malicious software having a characteristic unknown to said first sub-system, the activation for causing a consequence of the activation in said first sub-system, thereafter detecting the activated unknown malicious software in said first sub-system by detecting the consequence of the activation in said first sub-system of the unknown malicious software caused by the partial simulation (column 6, lines 63-67 and column 7, lines 1-18, "data is put into the emulation chamber 48 where the virus is fooled into acting as if it were really present on the host system. It is desired that any disruptive behavior the virus is capable of displaying take place in emulation chamber 48 such as replicating, attacking another program or destroying data" and lines 48-52),

and giving an alarm when a malicious software is detected (Figures 1 and 6C, column 8, lines 27-35, "Upon detection of a virus by the analysis and detection means 50, response/alarm means 52 can execute any number of user definable optional commands such as messaging or beeping a system administrator, notifying the sender and receiver of the file or program, deleting the file..." and lines 50-59).

10. Regarding 26, Schnurer teaches wherein the consequence of activation of the malicious software includes *at least one of*:

a change takes place in the first sub-system prior to actions causing changes carried out by the first sub-system, a change takes place in the first sub-system that is not an action taken by the first sub-system to detect a malicious software, a message leaves for another system without command from the first sub-system, a message leaves for another system to a wrong address or to a system which no communication has been directed to, and a message does not leave for another system although it has been sent there (column 6, lines 63-67 and column 7, lines 1-18, "data is put into the emulation chamber 48 where the virus is fooled into acting as if it were really present on the host system. It is desired that any disruptive behavior the virus is capable of displaying take place in emulation chamber 48 such as replicating, attacking another program or destroying data" and lines 48-67, "The first step is to determine whether the IRQ table was modified. The second step is to determine if another program was written to." and "It is the combination of grabbing one or more IRQs and attempting changes to either the FAT or executables that allows virus activity to be detected").

11. Regarding claim 29, Schnurer teaches further comprising the step of searching for known malicious software on the basis of its characteristics (column 7 lines 48-67, "The first step is to determine whether the IRQ table was modified. The second step is to determine if another program was written to." and "It is the combination of grabbing one or more IRQs and attempting changes to either the FAT or executables that allows

virus activity to be detected" and column 8, lines 3-14, "allowing a virus to be detected by its 'signature'").

12. Regarding claim 31, Schnurer discloses an apparatus for repelling a malicious software, comprising equipment for saving data and for handling data and equipment for transferring data with another apparatus, wherein the apparatus is configured to receive a message and to detect in the apparatus an unknown malicious software contained in the message and having a characteristic unknown to the apparatus, the apparatus being configured to perform a partial simulation in the apparatus to activate the unknown malicious software having a characteristic unknown to the apparatus and contained in the message, the activation causing a consequence of the activation in the apparatus, and thereafter the apparatus detecting the activated unknown malicious software by detecting the consequence of the activation of the unknown malicious software in the apparatus (column 6, lines 63-67 and column 7, lines 1-18, "data is put into the emulation chamber 48 where the virus is fooled into acting as if it were really present on the host system. It is desired that any disruptive behavior the virus is capable of displaying take place in emulation chamber 48 such as replicating, attacking another program or destroying data" and lines 48-52).

13. Regarding claim 33, Schnurer discloses wherein the consequence of activation of the malicious software includes *at least one of*: a change takes place prior to actions caused by changes made by the apparatus, a change takes place that is not an action taken by the apparatus to detect a malicious software (column 6, lines 63-67 and column 7, lines 1-18, "data is put into the emulation chamber 48 where the virus is

fooled into acting as if it were really present on the host system. It is desired that any disruptive behavior the virus is capable of displaying take place in emulation chamber 48 such as replicating, attacking another program or destroying data" and lines 48-67, "The first step is to determine whether the IRQ table was modified. The second step is to determine if another program was written to." and "It is the combination of grabbing one or more IRQs and attempting changes to either the FAT or executables that allows virus activity to be detected").

14. Regarding claim 37, Schnurer discloses wherein the apparatus examines the message in order to detect known malicious software (column 7, lines 48-67 and column 8, lines 3-14, "allowing a virus to be detected by its 'signature'").

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

The factual inquiries set forth in *Graham v. John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

Claims 3-6, 9, 15-17, 19-21, 30, 33, 34, 40 and 41 are rejected under 35 U.S.C. 103(a) as being unpatentable over United States Patent No. 5,842,002 to Schnurer et al., hereinafter Schnurer and further in view of United States Patent Application Publication No. US 2002/0116639 to Chefalas et al., hereinafter Chefalas.

15. Schnurer significantly discloses the claimed invention, as cited above. However, Schnurer fails to substantially disclose the claim limitations found within dependent claims 3-6, 9, 15-17, 19-21, 30, 34, 40 and 41. Chefalas discloses these claim limitations, as cited below.

16. Regarding claim 3, Chefalas discloses the security system in accordance with claim 1, configured to break a connection to at least one other system on the basis of an alarm caused by the detection of the malicious software (page 1, paragraph 12, page 2, remainder of paragraph 12 and paragraph 28, "VSC 126 at server 106 immediately severs the connection with client 112 and all other clients connected to the server", page 3, remainder of paragraph 28 and paragraphs 30 and 32 and page 4, paragraph 46).

17. The motivation to combine would be "for automatic detection, notification and elimination of viruses for a large network of machines" (*Chefalas* – page 1, paragraph 12).

18. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the teachings of Chefalas with the teachings of Schnurer so that "the proposed invention does not require manual intervention and

can act quickly and effectively to prevent viruses from spreading across the network of machines" (*Chefalas* – page 1, paragraph 12).

19. Regarding claim 4, Chefalas discloses a second sub-system for forwarding messages from the first sub-system to at least one system connected to the security system (page 3, paragraph 32, "If the same type of virus occurs several times in a specified time interval, server 106 sends a priority business event to the remote network administrator at server 108").

20. The motivation to combine would be "to coordinate activity and receive events from the virus scanner and notifier module located at clients 110-118 on the network" (*Chefalas* – page 2, paragraph 27).

21. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the teachings of Chefalas with the teachings of Schnurer so that "if a virus is detected on a client, such as client 112, software agent, VSN 128, installed on the client 112 immediately quarantines the offending file and notifies VSC 126 at server 106 via network 104 that a virus has been detected." (*Chefalas* – page 2, paragraph 28).

22. Regarding claim 5, Chefalas discloses a third sub-system configured to break a connection to at least one other sub-system upon receiving an alarm (page 1, paragraph 12, page 2, remainder of paragraph 12 and paragraph 28, "VSC 126 at server 106 immediately severs the connection with client 112 and all other clients connected to the server", page 3, remainder of paragraph 28 and paragraph 30, page 4, paragraph 46 and page 5, paragraph 54).

23. The motivation to combine would be that "if the detected virus is the type of virus that can be replicated or cloned, VSC 126 at server 106 immediately severs the connection with client 112 and all other clients connected to the server" (*Chefalas* – page 2, paragraph 28).

24. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the teachings of *Chefalas* with the teachings of Schnurer in order "to prevent further spreading of the virus in the case the virus has been sent to the server" (*Chefalas* – page 5, paragraph 54).

25. Regarding claim 6, *Chefalas* discloses wherein the at least one other sub-system includes an identifier which corresponds to an identifier of the third sub-system (page 4, paragraphs 44, 45 and 47 and page 5, paragraph 58).

26. The motivation to combine would be "to coordinate activity and receive events from the virus scanner and notifier module located at clients 110-118 on the network" (*Chefalas* – page 2, paragraph 27).

27. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the teachings of *Chefalas* with the teachings of Schnurer so that "if a virus is detected on a client, such as client 112, software agent, VSN 128, installed on the client 112 immediately quarantines the offending file and notifies VSC 126 at server 106 via network 104 that a virus has been detected." (*Chefalas* – page 2, paragraph 28).

28. Regarding claim 9, *Chefalas* discloses wherein the third sub-system includes at least one computer or one network element including a computer (page 3, paragraph

32. "If the same type of virus occurs several times in a specified time interval, server 106 sends a priority business event to the remote network administrator at server 108").

29. The motivation to combine would be "to coordinate activity and receive events from the virus scanner and notifier module located at clients 110-118 on the network" (*Chefalas* – page 2, paragraph 27).

30. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the teachings of *Chefalas* with the teachings of Schnurer so that "if a virus is detected on a client, such as client 112, software agent, VSN 128, installed on the client 112 immediately quarantines the offending file and notifies VSC 126 at server 106 via network 104 that a virus has been detected." (*Chefalas* – page 2, paragraph 28).

31. Regarding claim 15, *Chefalas* discloses further comprising a parallel system that saves a message sent from the third sub-system, the parallel system being connected in parallel with the third sub-system (page 1, paragraph 12, page 3, paragraph 30 and page 5, paragraph 54).

32. The motivation to combine would be to produce "rules that may be used to implement business decisions as to how to handle the notification of the presence of a virus within a network data processing system" (*Chefalas* – page 4, paragraph 46).

33. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the teachings of *Chefalas* with the teachings of Schnurer so that "the event is logged and then used as a metric to calculate production efficiency, downtime, failure to adhere to company policies against

downloading potentially harmful content or executing harmful programs" (*Chefalas* – page 5, paragraph 59).

34. Regarding claim 16, Chefalas discloses wherein the first sub-system compares in the parallel system a message sent from the third sub-system to the first sub-system and additionally saved in the parallel system in order to detect an anomaly caused by a malicious software (page 1, paragraph 12, page 3, paragraph 30 and page 5, paragraph 54).

35. The motivation to combine would be "to coordinate activity and receive events from the virus scanner and notifier module located at clients 110-118 on the network" (*Chefalas* – page 2, paragraph 27).

36. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the teachings of Chefalas with the teachings of Schnurer so that "if a virus is detected on a client, such as client 112, software agent, VSN 128, installed on the client 112 immediately quarantines the offending file and notifies VSC 126 at server 106 via network 104 that a virus has been detected." (*Chefalas* – page 2, paragraph 28).

37. Regarding claim 17, Chefalas discloses wherein the parallel system forwards a message saved by it (page 1, paragraph 12, page 3, paragraph 30 and page 5, paragraph 54).

38. The motivation to combine would be "to coordinate activity and receive events from the virus scanner and notifier module located at clients 110-118 on the network" (*Chefalas* – page 2, paragraph 27).

39. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the teachings of *Chefalas* with the teachings of Schnurer so that “if a virus is detected on a client, such as client 112, software agent, VSN 128, installed on the client 112 immediately quarantines the offending file and notifies VSC 126 at server 106 via network 104 that a virus has been detected.”

(*Chefalas* – page 2, paragraph 28).

40. Regarding claim 19, *Chefalas* discloses the security system in accordance with claim 4, comprising first and second ones of the at least one system, wherein the security system transfers data between the first and the second ones of the at least one system through the first and the second sub-systems, and wherein the security system disrupts the connection between the first one of the at least one system and the first sub-system before a connection is established between the first and the second sub-systems and disrupts the connection between the first and the second sub-systems before a connection is established between the second sub-system and the second one of the at least one system (page 1, paragraph 12, page 3, paragraph 30, “shut down the local server and/or the LAN” and page 5, paragraph 54).

41. The motivation to combine would be that “if the detected virus is the type of virus that can be replicated or cloned, VSC 126 at server 106 immediately severs the connection with client 112 and all other clients connected to the server” (*Chefalas* – page 2, paragraph 28).

42. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the teachings of *Chefalas* with the teachings

of Schnurer in order "to prevent further spreading of the virus in the case the virus has been sent to the server" (*Chefalas* – page 5, paragraph 54).

43. Regarding claim 20, *Chefalas* discloses wherein said first sub-system compares messages with at least partially identical identifiers with each other in order to detect the unknown malicious software (page 4, paragraphs 44, 45 and 47 and page 5, paragraph 58).

44. The motivation to combine would be "to coordinate activity and receive events from the virus scanner and notifier module located at clients 110-118 on the network" (*Chefalas* – page 2, paragraph 27).

45. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the teachings of *Chefalas* with the teachings of Schnurer so that "if a virus is detected on a client, such as client 112, software agent, VSN 128, installed on the client 112 immediately quarantines the offending file and notifies VSC 126 at server 106 via network 104 that a virus has been detected."
(*Chefalas* – page 2, paragraph 28).

46. Regarding claim 21, *Chefalas* discloses wherein the first sub-system requests the sender of the messages with at least partially identical identifiers to re-send at least one of the messages and further compares at least one re-sent message received with the original messages in order to detect messages containing the malicious software (page 4, paragraphs 44, 45 and 47 and page 5, paragraph 58).

47. The motivation to combine would be "to coordinate activity and receive events from the virus scanner and notifier module located at clients 110-118 on the network" (*Chefalas* – page 2, paragraph 27).

48. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the teachings of *Chefalas* with the teachings of Schnurer so that "if a virus is detected on a client, such as client 112, software agent, VSN 128, installed on the client 112 immediately quarantines the offending file and notifies VSC 126 at server 106 via network 104 that a virus has been detected." (*Chefalas* – page 2, paragraph 28).

49. Regarding claim 30, *Chefalas* teaches wherein the security system is connected to a first system and a second system and wherein data are transferred between the first system and the second system through the first sub-system and a second sub-system phase by phase in order (page 1, paragraph 12 and page 5, paragraph 54), in which phases:

the connection for data transfer is disrupted between the first system and the first sub-system, a connection for data transfer is established between the first sub-system and the second sub-system, the connection for data transfer is disrupted between the first sub-system and the second sub-system, a connection for data transfer is established between the second sub-system and the second system (page 5, paragraph 54).

50. The motivation to combine would be that "if the detected virus is the type of virus that can be replicated or cloned, VSC 126 at server 106 immediately severs the

connection with client 112 and all other clients connected to the server" (*Chefalas* – page 2, paragraph 28).

51. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the teachings of *Chefalas* with the teachings of Schnurer in order "to prevent further spreading of the virus in the case the virus has been sent to the server" (*Chefalas* – page 5, paragraph 54).

52. Regarding claim 34, *Chefalas* discloses wherein the apparatus sends a message to either a sub-assembly of the apparatus or to said another apparatus (page 3, paragraph 32, "If the same type of virus occurs several times in a specified time interval, server 106 sends a priority business event to the remote network administrator at server 108"), and wherein the consequence of activation of the malicious software includes *at least one of*:

a message leaves without authorization from the anti-malicious software of the apparatus, a message leaves for an address it has not originally been directed to, a message does not leave although it has been given a command to be sent (page 2, paragraphs 25 and 28, page 3, remainder of paragraph 28 and paragraphs 30-32 and page 4, paragraphs 44, 46 and 47).

53. The motivation to combine would be "to coordinate activity and receive events from the virus scanner and notifier module located at clients 110-118 on the network" (*Chefalas* – page 2, paragraph 27).

54. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the teachings of *Chefalas* with the teachings

of Schnurer so that "if a virus is detected on a client, such as client 112, software agent, VSN 128, installed on the client 112 immediately quarantines the offending file and notifies VSC 126 at server 106 via network 104 that a virus has been detected."

(*Chefalas* – page 2, paragraph 28).

55. Regarding claim 40, Chefalas discloses wherein the security system communicates with the computer network being protected by the security system, but is separate from the computer network (page 1, paragraph 12 and page 3, paragraph 32, "If the same type of virus occurs several times in a specified time interval, server 106 sends a priority business event to the remote network administrator at server 108").

56. The motivation to combine would be that "if the detected virus is the type of virus that can be replicated or cloned, VSC 126 at server 106 immediately severs the connection with client 112 and all other clients connected to the server" (*Chefalas* – page 2, paragraph 28).

57. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the teachings of Chefalas with the teachings of Schnurer in order "to prevent further spreading of the virus in the case the virus has been sent to the server" (*Chefalas* – page 5, paragraph 54).

58. Regarding claim 41, Chefalas discloses wherein the security system is in a gateway for the computer network (page 1, paragraph 12, page 3, paragraph 32, "If the same type of virus occurs several times in a specified time interval, server 106 sends a priority business event to the remote network administrator at server 108" and page 5, paragraph 59, "firewalls, servers or monitoring devices").

59. The motivation to combine would be "to coordinate activity and receive events from the virus scanner and notifier module located at clients 110-118 on the network" (*Chefalas* – page 2, paragraph 27).

60. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the teachings of *Chefalas* with the teachings of Schnurer so that "if a virus is detected on a client, such as client 112, software agent, VSN 128, installed on the client 112 immediately quarantines the offending file and notifies VSC 126 at server 106 via network 104 that a virus has been detected." (*Chefalas* – page 2, paragraph 28).

Claim Objections

61. Claims 22 and 23 are objected to because of the following informalities: did not properly indicate an amendment to the claims. The previous set of claims submitted on 9/22/08 contained the amended claim language of, "for repelling a malicious software". However, the amendments submitted on 5/26/09 omit the "a" without indicating that it has been removed (i.e. no double brackets). Appropriate correction is required.

Response to Arguments

62. The previous notice of non-compliance within the office action mailed on 12/23/08 is hereby withdrawn due to the Applicants submission of the corrected claims.

63. Applicant's arguments with respect to claims 1-6, 8-10, 12, 14-23, 26, 29-31, 33, 34, 37, 40 and 41 have been considered but are moot in view of the new ground(s) of rejection.

Conclusion

64. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

65. The following United States Patents and Patent Application Publication are cited to further show the state of the art with respect to virus detection and removal, such as:

United States Patent No. 7,137,034 to Largman et al., which is cited to show a self repairing computer having user accessible switch for modifying bootable storage device configuration to initiate repair.

United States Patent No. 6,873,988 to Hermann et al., which is cited to show system and methods providing anti-virus cooperative enforcement.

United States Patent No. 7,089,589 to Chefalas et al., which is cited to show a method and apparatus for the detection, notification and elimination of certain computer viruses.

United States Patent No. 7,171,690 to Kouznetsov et al., which is cited to show a wireless malware scanning back-end system and method.

United States Patent No. 7,096,381 and United States Patent Application Publication No. US 2002/0194534 to Largman et al., which are cited to show on-the-fly repair of a computer.

United States Patent Application Publication No. US 2004/0030913 to Liang et al., which is cited to show a system and method for computer protection against malicious electronic mails by analyzing, profiling and trapping the same.

United States Patent No. 7,140,041 to Jeffries et al., which is cited to show detecting dissemination of malicious programs.

United States Patent No. 7,058,822 to Edery et al., which is cited to show malicious mobile code runtime monitoring system and methods.

United States Patent No. 5,963,731 to Sagawa et al., which is cited to show a method of assisting execution of plural simulation programs for coupled simulation.

United States Patent No. 7,290,282 to Renert et al., which is cited to show reducing false positive computer virus detections.

66. Any inquiry concerning this communication or earlier communications from the examiner should be directed to JEREMIAH AVERY whose telephone number is (571)272-8627. The examiner can normally be reached on Monday thru Friday 8:30am-5pm.

67. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, William Korzuch can be reached on (571) 272-7589. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

68. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Jeremiah Avery/
Examiner, Art Unit 2431

/Syed Zia/

Primary Examiner, Art Unit 2431